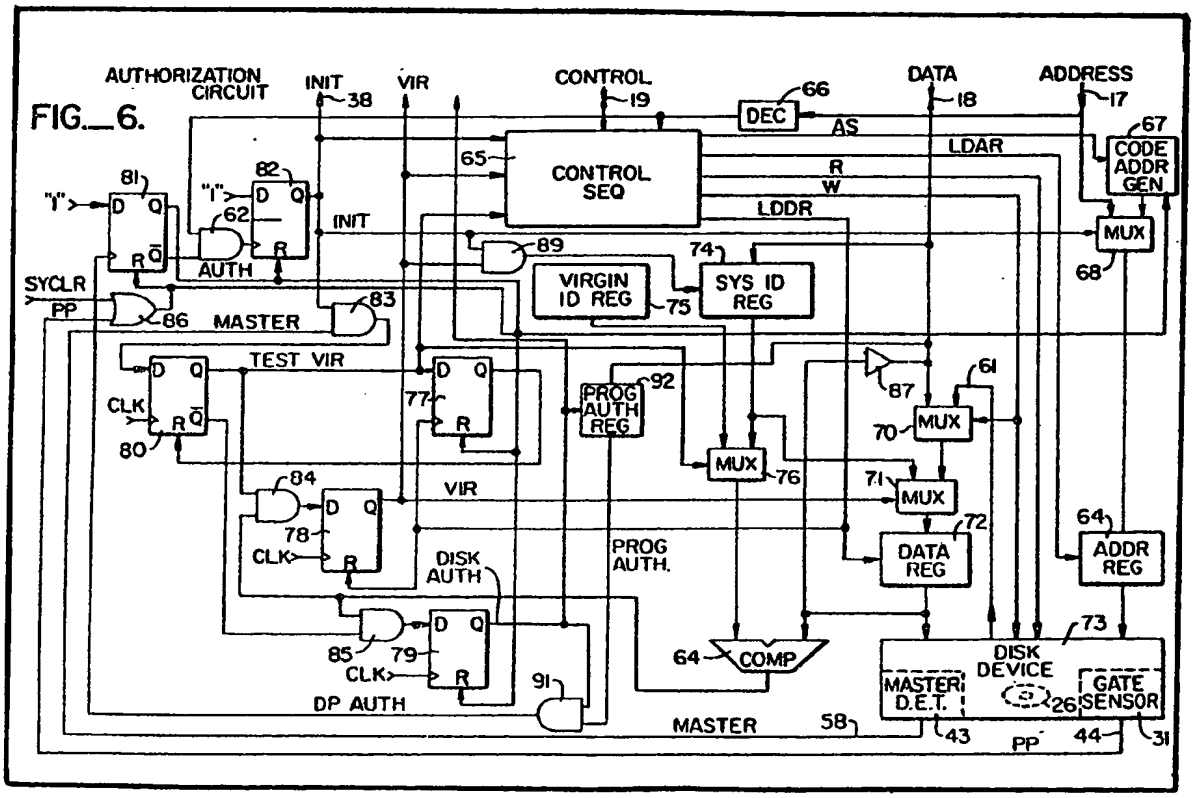
(12) UK Patent Application (19) GB (11) 2 123 597 A

(21) Application No 8315640
(22) Date of filing 7 Jun 1983
(30) Priority data
(31) 385480
(32) 7 Jun 1982
(33) United States of America (US)
(43) Application published 1 Feb 1984
(51) INT CL³ G06F 11/30 G11B 26/04 31/00
(52) Domestic classification G5R B264 B345 B36Y B421 B452 B482 B685 B687 B68X B781 B784 HB G4A 13E 16J 17B 1C 5B AP U1S 2119 G4A G5R
(56) Documents cited GB 1537759 GB 1525292 GB 1329721 GB 1255300 GB 1142465 GB A 2113432 GB A 2112971 EP A 0067875
(58) Field of search G5R G3A
(71) Applicant Fortune Systems Corporation, (USA—California), 1501 Industrial Road, San Carlos, California, United States of America
(72) Inventors Hubal Toth, Arpad Paul Toth
(74) Agent and/or address for service Lloyd Wise, Tregear and Co., Norman House, 105—109 Strand, London, WC2R 0AE

(54) Computer program protection

(57) In a digital computer system adapted according to the invention, a program disc is installed (73) and a program protection signal is generated (31) when the disc should be interrogated to determine whether it is authorised for use in the system. In response to such a signal the disc is interrogated by reading data from the disc and comparing (64) this data with a system identifier. If the data and the identifier match, a second signal is generated indicating that the disc is authorised. The system identifier is typically stored in a register (74) forming part of the system. The system can also be adapted (43) to identify a master disc, and whether the disc is virgin or non-virgin.



GB 2 123 597 A

The drawings originally filed were informal and the print here reproduced is taken from a later filed formal copy.

2123597

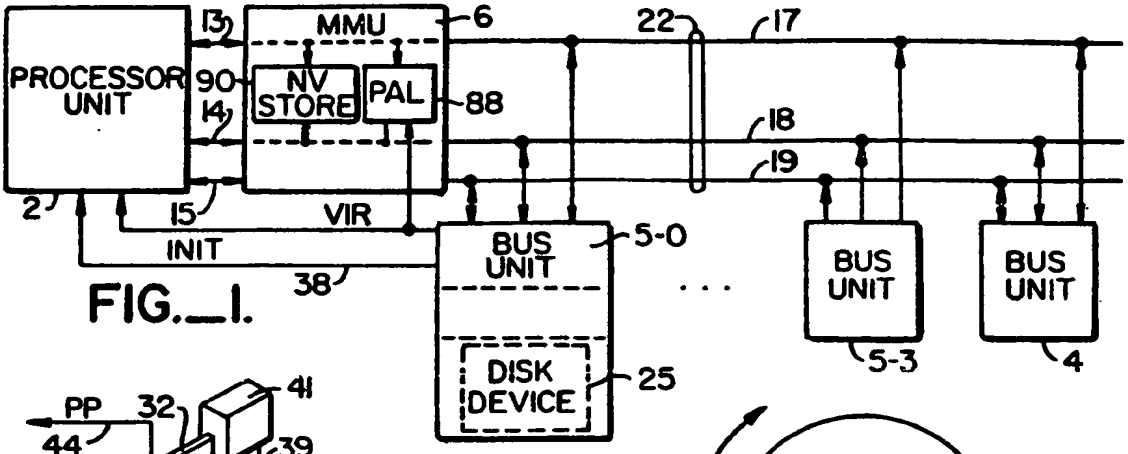


FIG._1.

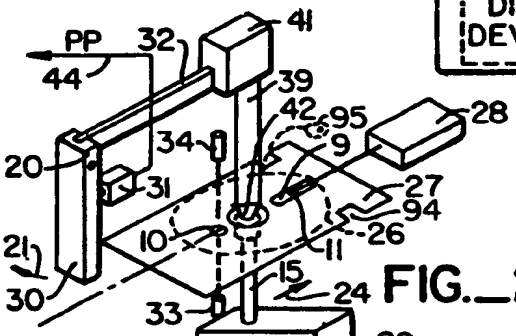


FIG._2.

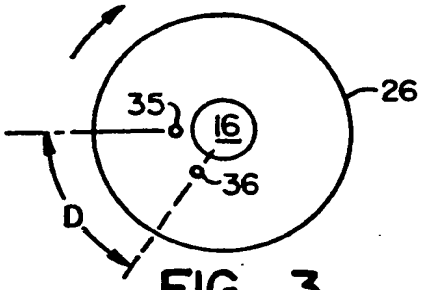


FIG._3.

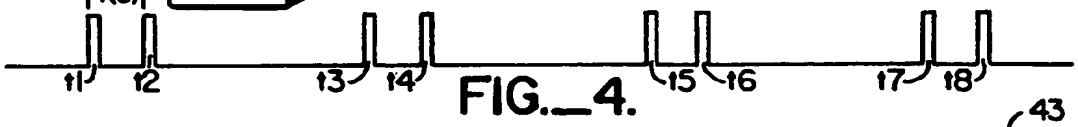


FIG._4.

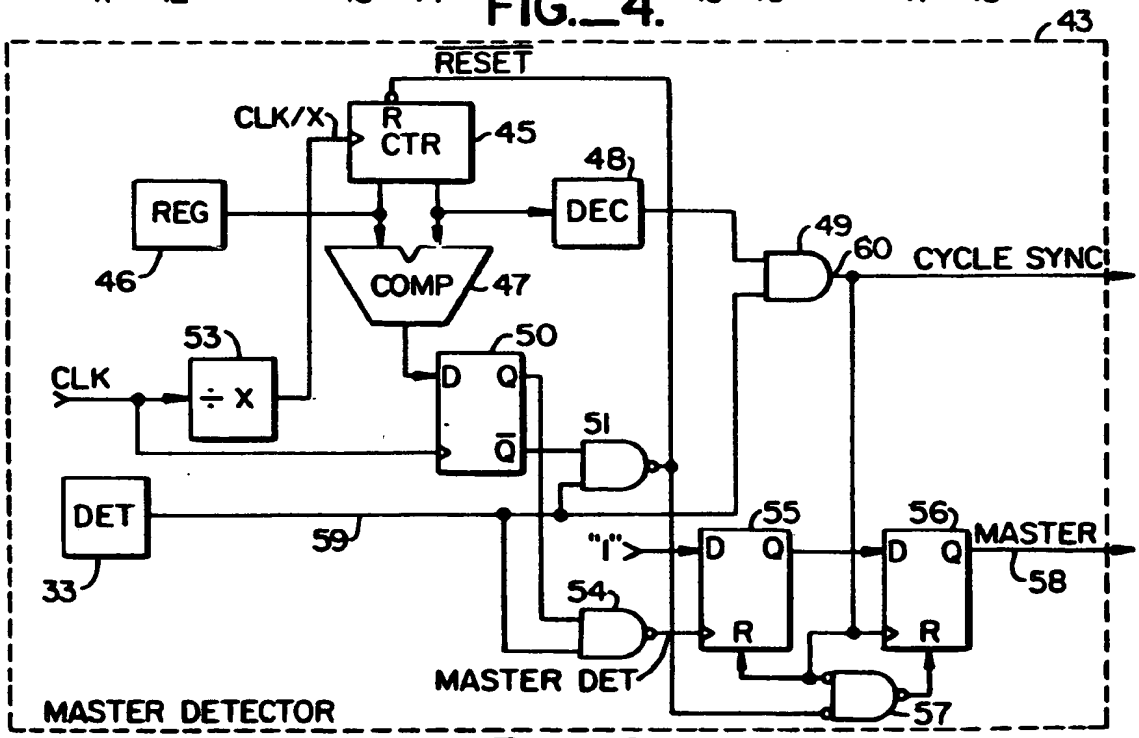


FIG._5.

2123597

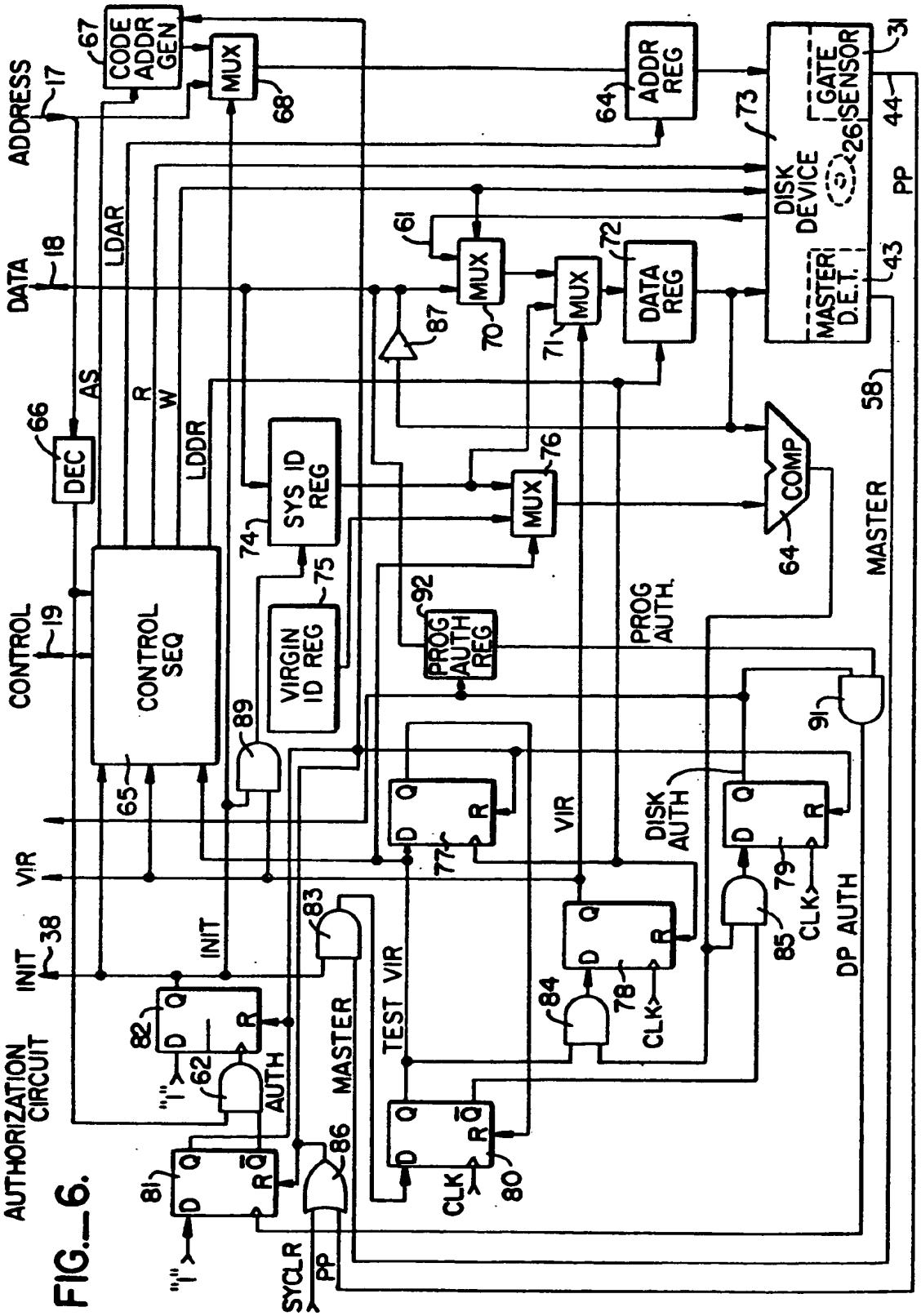


FIG._6.

SPECIFICATION

Computer program protection method and apparatus

The present invention relates to the field of digital computers and specifically to program protection methods and apparatus forming part of such computers.

Program protection is for ensuring that computer software is authorized to be used with a particular computer system. Before a system will accept a computer program, it is desirable to have the computer system check, through program protection methods, to ensure that the program is authorized. For purposes of this application, the term "program protection" is intended to mean the methods and apparatus which function to ensure that the computer system will accept and utilize only the properly authorized computer software.

The need for program protection arises for a number of reasons. One need for program protection arises when a computer system requires software with special features particularly adapted for the system. If a computer program has not been specially adapted to run on the computer system, then the running of the computer software may cause unwanted errors. Program protection is also desirable to ensure that computer programs have been properly tested before they are permitted to run on the computer system.

Only computer programs which have required features and which have been properly tested will be authorized.

Another need for software protection occurs in order to facilitate the marketing of computer software. Frequently, computer programs are marked under license to run only on a particular hardware system. Under such circumstances, there is a need to identify whether or not the computer program is authorized for a particular computer system. If an attempt is made to load an unauthorized computer program, the computer system should reject that program.

Another need for program protection arises to distinguish between different versions of computer programs. For example, an original program may differ substantially from new releases of a program containing updates and improvements. Such new releases may require special hardware features or may require a special fee before authorization is proper.

In addition to the foregoing, those skilled in the field of computers will recognize that other reasons exist for having program protection in data processing systems.

For many computer systems, computer programs are stored and delivered to users of computer systems on magnetic media. Frequently, the magnetic media are flex-discs since they are small, light-weight and easily transportable. Flex-discs have obtained widespread usage in the marketing of computer programs. Because magnetic discs are readily reproducable in copies and are readily modifiable, they have presented substantial problems when program protection has been desired.

Various methods have been proposed for protecting computer software particularly when the software is stored on magnetic discs. Such protection methods have not provided adequate flexibility for authorized uses nor sufficient protection from unauthorized uses.

In accordance with the above background, it is the objective of the present invention to provide improved program protection methods and apparatus for use in data processing systems.

The present invention is computer program protection methods and apparatus in computer systems. The protection apparatus includes disc sensing means for generating a program protection signal whenever a magnetic disc is newly engaged for use in the system. Whenever a disc is newly engaged in the system, the disc is interrogated to ascertain whether or not the disc is authorized for use on the computer system. If the disc is not authorized, the system will not accept the disc. If the disc is authorized, the disc is accepted for normal use.

In accordance with one feature of the invention, a master disc detector is provided for determining whether or not a newly engaged magnetic disc is a master disc. Master discs are of two types, virgin or non-virgin. A virgin master disc is one that does not have an authorization identifier for any authorized user system. A virgin master disc can be authorized for use on any properly authorized system. When a master disc is newly engaged in the system, it is tested to determine whether the master is a virgin or non-virgin. If the master disc is a virgin, then the system functions to store an authorize system identifier on the disc. Once the authorization system identifier has been stored on the disc, the disc is no longer a virgin and has become a non-virgin master. Thereafter, whenever the disc is loaded into the authorizing system, the system checks and ascertains that the disc is authorized to run on the system.

If a disc is not a master, the disc may be an authorized copy of a master which is authorized to run on the system. Whenever a disc is newly engaged in the system and the master detector determines that the disc is not a master, the system checks to determine whether or not the disc is an authorized copy. If the disc is an authorized copy, the system is enabled to access the disc for normal reading or writing of information.

Whenever a particular program is to be accessed on a disc which is an authorized disc, the program is checked to see if the program is authorized for use on the computer system. If the program is authorized, and the disc is authorized, then the system is permitted to access the disc and the computer program stored thereon.

In accordance with the above summary, the present invention achieves the objection of providing a program protection method and

apparatus which facilitates a distribution of authorized computer programs on authorized discs while preventing the use of unauthorized programs and discs.

The foregoing and other objects, features and advantages of the invention will be apparent from the following more particular description of preferred embodiments of the invention as illustrated in the accompanying drawings.

Fig. 1 depicts an overall data processing system in accordance with the present invention.

Fig. 2 depicts a schematic representation of a disc assembly for engaging and driving a flex-disc to read and write data in the operation of the Fig. 1 system.

Fig. 3 depicts a flex-disc, including both a timing indicator and an authorization indicator for a master disc.

Fig. 4 depicts a waveform representative of the output from a indicator detector for a master disc of the Fig. 3 type operating in the assembly of Fig. 2.

Fig. 5 depicts an electrical schematic representation of a master disc detector utilized in the Fig. 1 system.

Fig. 6 depicts a schematic electrical representation of an authorization circuit for detecting authorized magnetic discs in the Fig. 1 system.

Overall system—Fig. 1

In Fig. 1, the processing unit 2 connects to a memory management unit (MMU) 6 to a central logic bus (CLB) 22. The central logic bus 22 includes address bus 17, data bus 18 and control lines 19. The processor 2 also receives a first level interrupt signal, INIT, and a second level interrupt signal, VIR, from the bus unit 5-0. These interrupt signals are utilized in connection with the program protection mechanism.

In Fig. 1, a plurality of bus units 4 and 5-0,..., 5-3 connect to the central logic bus 22. Typically, the bus unit 4 is a random access memory which functions as a main store memory for the data processing system of Fig. 1. The bus units 5-0 through 5-3 typically include input/output devices such as keyboards, flex-discs, and hard-disc storage devices, parallel input/output devices, processing units and other types of units.

In Fig. 1, the bus unit 5-0 includes a flex-disc device 25 and conventional control circuitry for interfacing the flex-disc device 25 with the Fig. 1 system.

The flex-disc device 25 and bus unit 5-0 are employed in the system for loading computer programs into the system. The system is designed to accept only those discs and programs that are authorized for use in the Fig. 1 system.

In Fig. 1, a programmable array logic unit 88 is included within the unit 6. The unit 88 receives each address on address bus 17 and responsively, in accordance with some predetermined algorithm and/or encoding, provides an encoded output on the data bus 18. The output on bus 18 is a system identifier. The system identifier is stored in the authorization data field of a virgin flex-disc to thereafter enable the system to read from the disc.

Disc drive assembly—Fig. 2

In Fig. 2, a schematic representation of the flex-disc drive assembly which forms part of the flex-disc device 25 of Fig. 1 is shown. The flex-disc 26, indicated by broken line, is contained within a protective jacket 27. The disc 26 is free to move within the jacket 27. The jacket 27 and the disc 26 are inserted together in the direction of arrow 24 into the drive assembly of Fig. 2. In order to insert the jacket 27 and disc 26 into the assembly of Fig. 2, the gate 30 must be raised, in the direction of arrow 21, around the pivot 20 in order to provide clearance for insertion or retraction of the disc 26 and jacket 27.

The disc assembly of Fig. 2 includes detection apparatus, in the form of a switch 31, for sensing if a flex-disc has been newly engaged in the system. When gate 30 is raised, the switch 31 provides a program protection signal PP on line 44. The PP signal indicates that the gate 30 has been opened and, therefore, an unauthorized disc may have been inserted into the flex-disc device 25. The program protection signal initiates an interrogation to determine whether or not the inserted disc is authorized.

When the gate 30 is raised, the linkage 32 moves and causes member 39 to be retracted upwardly through operation of assembly 41. The upward movement of member 39 when the gate 30 is open retracts the tip 42 from the center indicator 16 of the disc 26. The tip 42 is rotably engaged to the member 39. When tip 42 is engaged in the indicator 16, it mates with a drive member at the end of the driveshaft 15 of motordrive 29. The motordrive 29, through the shaft 15 and the tip 42, clamps the disc 26 and drives it in a clockwise direction. A magnetic read-write head 11 reads and writes data from and to disc 26. Head 11 is moved back and forth by the head drive assembly 28. The head 11 is positioned over an opening in the jacket 27 and, therefore, has access directly to the surface of disc 26.

A hole 10 is located in the jacket 27 at some preselected radial position for exposing a timing track for disc 26. Referring to Fig. 3, the timing indicator 35 is shown in the timing track at a radial position which will align with the hole 10 in Fig. 2. The indicator 35 is conventionally a hole but can be any other type of indicator.

The jacket 27 has two parts, one above and one below the disc 26 in Fig. 2. The hole 10 extends through both the top and bottom parts of the jacket, so that when the indicator 35 is aligned with the hole 10, a light beam radiates all the way through jacket 27 and indicator 35 without being stopped.

In Fig. 2, an optical detector, including a light source 34 and a light detector 33, is positioned in alignment with the hole 10. The detector 33 operates to sense any indicator, such as the timing indicator 35, in the disc 26 when the

counter 45, gate 49 does not indicate that an output from decoder 48 has occurred.

The operation for the master detection circuit of Fig. 5 is as follows for a condition where the disc 26 of Fig. 3 is a master disc. When the pulse t1 of Fig. 4, resulting from indicator 35 of disc 26, causes a signal on line 59, the output from flip-flop 50 to gate 51 is a logical 1. Accordingly, the output from gate 51 is asserted, as a logical 0, to reset the counter 45. Counter 45 thereafter continues to count the clock pulses. Register 46 is stored with a count representing the position of the master indicator 36. When master indicator 36 is positioned to be detected by detector 33 and generates the t2 pulse of Fig. 4, comparator 47 is satisfied to provide a logical 1 to the flip-flop 50 causing the $\overline{Q}$ output of flip-flop 50 to be a logical 0. The logical 0 into NAND gate 51 prevents the t2 pulse on line 59 from asserting any output from NAND gate 51, and therefore, counter 45 is not reset by the operation of the t2 pulse.

The t2 pulse, however, is input to the NAND gate 54 along with the logical 1 from flip-flop 50 to assert the output of gate 54 as a logical 0 clocking a 1 into flip-flop 55. The 1 is stored in flip-flop 55 until counter 45 has advanced to the full cycle count detected by detector 48. The full cycle count from detector 48 together with the t3 pulse, generated by the second revolution of disc 26 and the alignment of indicator 35 with the detector 33, clocks the 1 from flip-flop 55 into flip-flop 56. At this time, the MASTER signal on line 58 signifies that disc 26 is a master. Flip-flop 56 is not reset by gate 57 as long as a master disc 26 is within the drive assembly of Fig. 2.

The operation of the Fig. 5 circuit when the disc 26 is not a master disc is as follows. At a time when the t1 pulse from indicator 35 occurs, flip-flop 50 is again clocked to have a 1 on its $\overline{Q}$ output so that the output from gate 51 is asserted to reset the counter 45. Assuming that the indicator 36 is either not present or is present at a location other than at the displacement "D", comparator 47 will provide, if at all, an output, to the flip-flop 50 at a time which does not correspond to a pulse on line 59. Accordingly, the NAND gate 54 is never asserted to gate a 1 on the Q output of flip-flop 55.

Under the condition that there is a second timing indicator 36 located, however, at other than the displacement "D", the operation of the Fig. 5 circuit is as follows. Each of the pulses t1, t2, t3,..., t8 on line 59 will cause the gate 51 to be satisfied to assert the $\overline{RESET}$ signal to reset the counter 45. Accordingly, counter 45 will not reach the full cycle count and hence decoder 48 will not assert an input to the AND gate 49. Accordingly, there will be no CYCLE SYNC signal on line 60. The line 60 signal remains a logical 0, which together with each output asserted from NAND gate 51, resets flip-flop 56 to ensure that the MASTER signal on line 58 is not asserted. If the absence of a CYCLE SYNC signal once-per-revolution indicates that an illegitimate master disc is in the system.

Under the condition where the disc 26 only has a single timing indicator 35, the operation of the Fig. 5 circuit is as follows. Each time the t1, t3, t5, and t7 signals appear on line 59, gate 51 is satisfied to assert the $\overline{RESET}$ signal to reset counter 45. The t2, t4, t6, and 58 pulses are not present since counter 45 is only reset once per cycle, decoder 48 provides an output at the same time as the signals are asserted from line 59 from detector 33. Therefore, the AND gate 49 becomes satisfied once per cycle to assert the CYCLE SYNC signal on line 60.

At the time that the count in counter 45 matches the master count in register 46, flip-flop 50 will be clocked to store a logical 1. However, since there is no corresponding pulse on line 59, when flip-flop 50 is clocked, NAND gate 51 is not satisfied, nor is NAND gate 54 satisfied. Accordingly, the output from comparator 47 in the absence of a timing pulse on line 59 corresponding to the master indicator 36, prevents counter 45 from being reset and prevents flip-flop 55 from being clocked to store a 1. The CYCLE SYNC signal on line 60 under this condition continuously resets the flip-flops 55 and 56. The assertion of a CYCLE SYNC signal on line 60 when no MASTER signal is asserted on line 58, indicates that the disc 26 may be an authorized copy of a master.

The decoder 48 is set to have a count which represents the number of incremental locations that exist when disc 26 makes one complete revolution. In one example, decoder 48 is set to a count of 252 and counter 45 is an 8-bit binary counter. The divide-by-X circuit 53 has the quantity "X" selected such that 252 clocking inputs will be provided to counter 45 for each single revolution of the disc 26. In the example where the displacement "D" is approximately 60 degrees, and decoder 48 is set to 252, then register 46 would store a count of 42.

In general, the sizes of the timing indicators 35 and 36 are selected to be greater than the dimension represented by a single count of counter 45. Accordingly, the actual diameter of indicator 36 would be selected such that its location is at a position represented by count 41, count 42, and count 43 of counter 45. Since the clock rate of flip-flop 50 is X-times greater than the clock rate of counter 45, flip-flop 50 will not miss detecting the master indicator 36. Of course, the size of the timing indicator 35 and 36, the number of counts represented in a full cycle (represented by the number decoded by decoder 48) and the location of the master indicator 36 relative to the timing indicator 35 (the contents of register 46) are all variables which can be determined as a function of the clock rate CLK and the angular velocity of the disc 26.

Authorization circuit—Fig. 6

In Fig. 6, further details of an authorization circuit are shown. The authorization circuit of Fig.

6 is part of the bus unit 5-0 of Fig. 1. The bus unit 5-0 of Fig. 1 includes a flex-disc device 25 and all of the control circuitry necessary to interface the flex-disc device 25 with the bus 22. Such control circuitry is standard and includes a number of conventional items. Referring to Fig. 6, the bus unit 5-0 includes a data register 72 in which data is transferred to and from the disc device 73. The disc device includes the drive assembly of Fig. 2. Register 73 receives data from the disc 26 through the buffer 87 and multiplexers 70 and 71. Data is stored in the data register 72 when register 72 is enabled by the load data register (LDDR) signal from a control and sequencer 65.

The location at which data is read from or stored at in the disc 26 is determined by the address register 69 of Fig. 6. Address register 69 is enabled to store an address by the load address register (LDAR) signal from the control and sequencer 65. The address stored in address register 69 is derived either from the CLBA address bus 17 which is one part of the CLB bus 22 of Fig. 1. The high-order address bits from bus 17 connect to the decoder 66 for indicating when the address space of bus unit 5-0 has been addressed. The low-order bits from bus 17 connect as an input to the multiplexer 68 for loading into the address register 69. The other input to the multiplexer 68 is from the code address generator 67. The code address generator 67 stores the addresses of the system identifier field and of the program name field locations on the disc 26.

The address generator is a read-only memory, counter or other device which outputs addresses in sequence. The generator is reset to the starting address when the reset signal from OR gate 86 is asserted. Generator 87 is stepped to a new address by assertion of the AS signal from control sequencer 65.

The multiplexer 68 selects the address from the code address generator 67 when the initialized (INIT) signal is asserted from the flip-flop 82. The CLBD bus 18 provides data to and from the bus unit 5-0. In Fig. 6, the bus provides one input to the multiplexer 70 which in turn provides an input to the multiplexer 71 which in turn provides an input to the data register 72.

Output data over the bus 18 comes from the buffer 87 which receives data output from the data register 72. The multiplexer 70 receives a second input for data from the disc 26 in the disc device 73. Data is selected from bus 18 for input to the multiplexer 71 and data register 72 when the write (W) signal from the control sequencer 65 is asserted. When the W signal is not asserted, multiplexer 70 selects data from the disc device 73 on bus 61.

Data on bus 18 is also input to the system identifier register 74 and the program authorization register 92. Register 74 stores the data from bus 18 when enabled by the output from AND gate 89 which receives the INIT and VIR signals. A system identifier stored in register 74 is selected by multiplexer 71 for storage in the data register 72 and for writing onto the disc 26. The selection by multiplexer 71 occurs when the virgin disc indicating signal, VIR, from flip-flop 78 is asserted. When VIR is not asserted, multiplexer 71 selects the output from multiplexer 70 for storage in data register 72. The system identifier from register 74 is also selected by multiplexer 76 as one input to the comparator 64 when the test virgin signal, TEST VIR, is not asserted on the Q output of flip-flop 80. When TEST VIR is asserted, then the virgin ID from the registers 75 is selected by multiplexer 76 as one input to the comparator 64. The other input to the comparator 64 is the output from the data register 72.

The function of comparator 64 is to compare the contents of data register 72 with a virgin ID from register 75 at a time when the TEST VIR signal has been asserted, and at other times to compare the contents of the data register 72 with the system identifier from register 74. When the contents compare, the output from comparator 64 is asserted to enable the AND gates 84 and 85.

In Fig. 6, the OR gate 86 receives the PP signal on line 44 from the gate sensor 31 to Fig. 2 and is shown schematically as part of the disc device 73 of Fig. 6. The OR gate 86 also receives a system clear signal, SYCLR, which is asserted for example whenever the power to the system of Fig. 1 is turned on. The SYCLR signal is also provided at any other time when the status of the registers and other storage devices may be in doubt. Whenever OR gate 86 is satisfied and its output is asserted, the authorization flip-flop 81 is reset to provide a 0 on its Q output and a 1 on its $\overline{Q}$ output.

If, after operation of the Fig. 6 circuit, the disc asserted in the assembly of Fig. 2 is an authorized disc, the DISC AUTH signal will enable AND gate 91. If the program stored on disc 26 is authorized for the system, then the output from register 92 will satisfy AND gate 91. The asserted output from gate 91 will enable flip-flop 81 to store a logical 1 on its Q output and a 0 on its $\overline{Q}$ output.

Whenever flip-flop 81 has been reset, for example, when the gate 30 of Fig. 2 has been opened to provide the PP signal on line 44, the AND gate 62 is enabled by a logical 1 from the $\overline{Q}$ output from flip-flop 81. Whenever the decoder 66 senses that the bus unit 5-0 (see Fig. 1) is addressed after AND gate 62 has been enabled, flip-flop 82 is clocked to store a logical 1 on its Q output and thereby assert the INIT signal. The assertion of the INIT signal functions to cause the circuit of Fig. 6 to determine whether or not the disc 26 is an authorized disc. The INIT signal is provided as an interrupt signal to the processor unit 2 of Fig. 1 over line 38.

Also, when the INIT signal is asserted, multiplexer 68 selects the code address from the generator 67 for storage in the address register 69. The INIT signal is also input to the control and sequencer 65 for initiating the output signals from sequencer 65 which cause the authorization checking functions to be performed by the Fig. 6

apparatus. The INIT signal is also input to the AND gate 83 which also receives as its other input the MASTER line from the master detector 43 of Fig. 5. If the authorization sequence is initiated by the flip-flop 82 asserting INIT, and the disc 26 is a master disc as indicated by the assertion of MASTER, gate 83 is satisfied to clock a logical 1 to the Q output of flip-flop 80. The Q output of flip-flop 80 when asserted provides the TEST VIR signal which causes the disc 26 to be tested to see if it is a virgin master disc.

The asserted TEST VIR signal enables the AND gate 84. The other input to gate 84 is the output of comparator 64. The asserted TEST VIR signal causes the multiplexer 76 to provide the virgin ID from register 75 as one input to comparator 64. If the contents of data register 72 are the same as the virgin ID, then the output from comparator 64 will satisfy AND gate 84 causing the VIR signal to be asserted on the Q output of flip-flop 78. When VIR is asserted indicating that the master disc in the assembly of Fig. 2 is a virgin, multiplexer 71 enables the system identifier from register 74 to be stored in the data register 72 for writing the system identifier onto the disc 26.

The system identifier has been previously loaded into the register 74 as a result of the interrupt caused to processor unit 2 when the INIT signal was asserted on line 38. At the time that the system identifier is stored in the data register 72 by energization of the enable signal LDDR from sequencer 65, the flip-flop 77 is clocked to store the TEST VIR signal. At the same time, the assertion of the LDDR signal resets the virgin flip-flop 78.

With the virgin ID stored in register 72, a write cycle is caused by the assertion of the W signal from the sequencer 65. The virgin ID is written onto the disc 26 at the address specified by the address register 69.

Thereafter, since the VIR signal is non-asserted, multiplexer 71 selects the output from multiplexer 70 as the input to the data register 72. The control sequencer causes a read cycle by assertion of the R line which causes the system identifier to be read from the disc device 73 and stored in the data register 72.

When the flip-flop 77 was clocked by the LDDR signal, it asserted its Q output to reset the flip-flop 80 thereby causing the TEST VIR signal to be non-asserted. The multiplexer 76 therefore provides the system identifier from register 74 is one input to comparator 64 along with the system identifier from data register 72 previously read from the disc 26. When comparator 64 asserts its output, AND gate 85 has been enabled when flip-flop 80 was reset, so that flip-flop 79 is clocked to assert the disc authorize signal DISC AUTH. The DISC AUTH signal clocks the flip-flop 81 and asserts the AUTH signal. The asserted AUTH signal resets the flip-flop 82 negating the INIT signal while resetting flip-flops 77 and 79. With INIT negated, the interrupt on line 38 is removed and the Fig. 6 circuit thereby indicates that the disc 26 is authorized to be accessed by the CLB bus 22. With the INIT signal negated, the multiplexer 68 connects the address bus 17 directly to the address register 69 and bus 18 connects to or from the data register 72.

In Fig. 6, the control sequencer 65 is a standard sequential logic device which operates in a conventional way to provide a number of sequential signals. Those signals include the LDAR signal for enabling the address register 69, the LDDR signal for enabling the data register 72, the W signal for commanding a write operation of the contents of data register 72 onto the disc 26, an R signal for providing a read operation for reading the contents of disc 26 into the data register 72, and an AS signal for incrementing the address generator 67. These signals are provided in a conventional manner for reading and writing data when the INIT signal has not been asserted. However, when the INIT signal is asserted, the control sequencer 65 provides a sequence of outputs for implementing a program protection mechanism. Which are explained in detail in connection with the following Table 1:

Table 1

$$
\begin{aligned}
\text{LDAR} &= (\text{INIT} * T1) \\
&+ [\text{Load AD Normal}] * \overline{\text{INIT}} \\
R &= (\text{TEST VIR} * \text{INIT} * T2) \\
&+ (\text{TEST VIR} * \overline{\text{VIR}} * \text{INIT} * T5) \\
&+ (\text{VIR} * T6 * \text{INIT}) \\
&+ [\text{Read Normal}] * \overline{\text{INIT}} \\
W &= (\text{VIR} * \text{INIT} * \text{LDDR} * T4) \\
&+ [\text{Write Normal}] * \overline{\text{INIT}} \\
\text{LDDR} &= (\text{VIR} * \text{INIT} * T3) \\
&+ (R * \text{INIT}) * (T2+T5+T6) \\
&+ [\text{Load DA Normal}] * \overline{\text{INIT}} \\
AS &= T1+T2+T3+T4+T5+T6
\end{aligned}
$$

In Table 1, the asterisk symbol "*" represents a logical AND and the plus symbol "+" represents a logical OR. In Table 1, the last line of each of the equations except for AS represents the normal operation when the initiation signal INIT has not been asserted. All of the other lines represent the operation of the sequencer when INIT has been asserted.

Disc authorization operation

The operation of the Fig. 6 circuit is described when gate 30 has been opened and a master disc 26 has been placed into the disc assembly of Fig. 2. When the gate 30 is open, the PP signal is received by the OR gate 86 to reset flip-flop 81. Flip-flop 81 enables AND gate 62 when the system of Fig. 1 addresses the bus unit 5-0, the decoder 66 causes AND gate 62 to be satisfied causing flip-flop 82 and asserting the INIT signal. With INIT asserted, the LDAR signal, as indicated in Table 1, is initiated at T1 loading the address register with the contents of the code address generator 67. The address in generator 67 is the address of the field at which the system identifier is stored on the disc 26. The INIT signal causes an interrupt to the processor unit 2 which in turn

causes the system identifier to be loaded into the generator 74 of Fig. 6 which is enabled to receive the system identifier because INIT is asserted.

The INIT signal and MASTER signals are asserted to satisfy gate 83, thereby causing the assertion of TEST VIR. The TEST VIR signal together with the INIT signal asserted, as indicated in Table 1, causes the R signal to be asserted at T2, thereby reading the contents of disc 26 of the address specified by register 69. The information read from disc 26 is stored into the data register 72 through multiplexers 70 and 71. The assertion of the R signal at T2 in the presence of the INIT signal, as indicated in Table 1, causes the LDDR signal to be asserted at T2 to enable the data register 72 to store the data from the disc 26. With TEST VIR asserted, multiplexer 76 selects the virgin ID from register 75 then compares it with the data in register 72. If the virgin ID from register 75 and the contents of register 72 are the same, then the comparator 64 has its output asserted to cause the assertion of VIR from flip-flop 78. If the contents of register 72 and 75 are not the same, then comparator 64 does not have an asserted output and the VIR signal will not be asserted.

In the example where the disc 26 is a virgin master, then the system identifier from register 74 is loaded into the data register 72. Data register 72 is loaded by the LDDR signal which, as shown in Table 1, is asserted at T3 when both VIR and INIT signals are asserted. When the LDDR signal at T3 causes the system identifier to be stored in the register 72, the write signal W, as seen in Table 1, is asserted at T4 to write the contents of data register 72 onto the disc 26. The loading of the register 72 with the system identifier, by the assertion of the LDDR signal at T3, negates the VIR signal. Under these conditions, the R signal is asserted at the T5 time to store the system identifier read from disc 26 in the data register 72. The LDDR signal is asserted at T6 time to store the data read from the disc into register 72.

At this time the contents of register 74 are compared with the system identifier contents of register 72 from the disc and, in the absence of an error condition they should compare. AND gate 85 is satisfied asserting the DISC AUTH signal which in turn enables the AND gate 91. If the program authorization register is also set, gate 91 will be satisfied to assert the AUTH signal from flip-flop 81. The AUTH signal negates the INIT signal and the disc 26 is ready for normal accessing by the system of Fig. 1.

In the example described where the disc was not a virgin and VIR from flip-flop 78 was never asserted, the system identifier in register 74 is never loaded into the register 72 and is not written onto the disc 26.

The operation of the Fig. 6 circuit when the master disc is not a virgin is as follows. When comparator 64 determines that the contents of the data register 72 are not the same as the contents of the register 75, the VIR signal is not asserted. The read operation at T2 which places the data in register 72 resets the flip-flop 77 and negates the TEST VIR signal after the next CLK. With VIR and TEST VIR negated, the multiplexer 76 is switched to select the output from the system identifier register 74 so that it is then compared with the contents of data register 72. If a comparison occurs, gate 85 is enabled and flip-flop 79 is clocked to assert the DISC AUTH signal. If the program is also authorized, the DISC AUTH signal satisfies AND gate 91 and that clocks flip-flop 81 to assert the AUTH signal and negate the INIT signal. When INIT is negated, the interrupt 38 is removed and the bus unit 5-0 of Fig. 1 is available for general use. This operation will occur for a non-virgin master disc. A non-virgin master disc is one which is already been authorized for use in the system of Fig. 1.

The operation of the Fig. 6 circuit when the disc 26 is not a master disc is as follows. If disc 26 is not a master, the MASTER signal will be negated and hence the output from AND gate 83 will not be asserted. Accordingly, TEST VIR and VIR will not be asserted. Accordingly, a read operation during the T5 time of Table 1 will read the data from the address specified by address register 69. The data from the addressed location in the disc 26 is stored in the data register 72. If the contents of register 72 from disc 26 are the same as the contents of the system identifier register 74, comparator 64 will assert its output and satisfy AND gate 85 which is clocked through flip-flop 79 to assert the DISC AUTH signal which, for an authorized program, in turn asserts the AUTH signal and nagates the INIT signal. Under this condition, with a logical 1 output from comparator 64, the disc 26 is an authorized copy of an authorized master. If the contents of data register 72 and 74 are not the same, then the output from comparator 64 will not be asserted and hence neither the DISC AUTH or the AUTH signals will be asserted. Hence the INIT signal will remain asserted and the interrupt on line 38 will not be removed. The processor unit 2 will recognize when the interrupt on line 38 is not removed within a sufficient period of time and will issue a program protection exception identifying that the disc engaged in the bus unit 5-0 is not authorized.

In the Fig. 1 system, the processor unit 2 functions to detect the interrupt on line 38 in a conventional manner. The address of the bus unit 5-0 which causes the interrupt on line 38 has been supplied by the processor unit 2 on the bus 17. When the programmable array logic unit 88 of Fig. 1 is enabled by the VIR signal, unit 88 responsively provides an output on the data bus 18. The output on data bus 18 is transmitted to the bus unit 5-0 and is stored in the system identifier register 74 by the output of AND gate 89 in the manner previously described.

In the example described, the array logic unit 88 is addressed by a single address sequence. However, multiple sequential addresses for addressing unit 88 can be required before the

proper output from unit 88 will occur. The use of multiple sequential addresses greatly enhances the protection provided against attempts at breaking the protection mechanism.

The programmable logic 88 provides the system identifier which is used to determine whether or not the disc 26 is an authorized disc. In the case of a virgin master disc, the programmable array logic 88 provides the system identifier which is stored on the disc to form a non-virgin master disc and thus authorize that disc, and any copies thereof for use on the system of Fig. 1. The programmable array logic 88 can perform any function on the input address on bus 17 to provide the system identifier on the output bus 18. In one example, the output on bus 18 can be identical to the address on bus 17 and hence the system identifier is merely the address of the programmable array logic 88.

Authorized program operation

In Fig. 1, the non-volatile store 90 is connected to be addressed by bus 17 to provide an output on data bus 18. The non-volatile store 90 is a device which is addressable by address bits on bus 17 to store information from bus 18 or to read out information to bus 18 depending upon the state of the VIR signal. When VIR is asserted, store 18 will receive information from bus 18 and store that information at the addressed location. When VIR is not asserted, store 90 only operates in the read mode and provides output data to the bus 18. The non-volatile store 90 functions to retain its information even if the power for the Fig. 1 system is turned off and then returned to on.

Store 90 is addressed for reading to determine whether or not the program contained on the disc has been authorized for the system of Fig. 1. In one example, the non-volatile store 90 includes an 8-bit field of program names where up to 256 different programs can be authorized for use with the Fig. 1 system. The high-order address bits on bus 17 are decoded to select the store 90 in a conventional manner and the low-order 8-bits of the address correspond to the possible program names on the disc. Store 90 is, therefore, an authorized program store which stores an indication for each program up to some maximum which is authorized.

When the INIT signal is sensed by the processor 2 and provided that the VIR signal is present, the processor unit 2 first addresses the programmable array logic 88 in Fig. 1 to access the system identifier. The system identifier is stored in the register 74 of Fig. 6 as previously described. Next, the processor 2 monitors the VIR signal and, if the VIR signal is present, it will update the non-volatile store 90 at the appropriate time. The appropriate time occurs after the T6 signal. If the VIR signal has been present, then the processor unit 2 carries out a WRITE operation in the non-volatile store 90. The low-order address bits are the program name from the disc 26. A logical one bit is stored into the non-volatile store at the program address determined when the program name is accessed from the data register 72 for a virgin master disc.

After a WRITE operation for a virgin master disc (VIR asserted) or directly for any non-virgin disc (VIR not asserted), the store 90 is read using the program name for the low-order address. The single bit of data, 1 or 0, is transmitted over bit 9 of bus 18 and stored in the program authorization register 92 to provide the PROG AUTH signal. If the program is properly authorized for the system, the register 92 will store a logical 1 and will thus satisfy the AND gate 91 provided the DISC AUTH signal has been asserted by flip-flop 79 in Fig. 6. If either the disc is not authorized, that is the DISC AUTH signal is not asserted, or the program is not authorized, that is the PROG AUTH signal from register 92 is not asserted, then the gate 91 will not be satisfied and the DP AUTH signal will not be asserted.

If either the disc is not authorized or the program is not authorized, flip-flop 81 will not be clocked to a 1 to assert the AUTH signal. If the AUTH signal is not asserted, then flip-flop 82 is not reset and the INIT signal remains asserted as an interrupt signal to the processor 2 on line 38. If the INIT signal is not removed within a predetermined time, then processor 2 recognizes that a program protection exception has occurred and will continue further processing without permitting access to the disc 26 for normal reading and writing.

Claims

1. In a computer system adapted for receiving computer program from a disc in a disc device, the program protection apparatus comprising:

detection apparatus for providing a program protection signal for indicating when a disc should be interrogated to determine if the disc is authorized for use in the system,

authorization means, responsive to said program protection signal for interrogating said disc, said authorization means including,

system identifier register means for storing a system identifier,

means for reading disc data from a predetermined field of said disc,

comparator means for comparing said disc data with said system identifier to provide an authorized signal when said disc authorization data and said system identifier are the same.

2. The program protection apparatus of Claim 1 wherein said authorization means further includes,

master detector means for providing a master signal when said disc is a master,

means for providing a virgin identifier,

means for causing disc data to be read from said predetermined field of said disc in response to said master signal,

comparator means for comparing said disc data with said virgin identifier to provide a virgin signal when said disc data and said virgin identifier are the same.

3. The program protection apparatus of Claim 2 further including,

means responsive to said virgin signal for writing said system identifier into said predetermined field of said disc whereby said disc becomes a non-virgin master.

4. The program protection appparatus of Claim 3 further including generator means for generating said system identifier in response to said virgin signal and means for storing said system identifier in said system identifier register.

5. The program protection apparatus of Claim 4 wherein said generator means includes programmable array logic for generating said system identifier as a function of an address used to address said disc unit by said system.

6. The program protection apparatus of Claim 5 wherein said master disc has a timing track with a timing indicator and with a master indicator angularly displaced from said timing indicator, and wherein said master detector has means for detecting the angular displacement of said master indicator relative to said timing indicator and means for determining whether said displacement corresponds to the displacement for a master disc.

7. The program protection apparatus of Claim 1 further including means for providing an initiation signal in response to said program protection signal for inhibiting the operation of said disc device for normal reading and writing of information until said authorization signal is generated.

8. The program protection apparatus of Claim 1 further including,

a program authorization store for storing program authorization identifiers to identify authorized programs for said system,

means for reading the name of a program on said disc,

means responsive to said name for determining if the program on said disc has an authorization identifier in said program authorization store.

9. The program protection apparatus of Claim 2 further including,

a program authorization store for storing program authorization identifiers to identify authorized programs for said system,

means for reading the name of a program on said disc,

means responsive to said name for determining if the program on said disc has an authorization identifier in said program authorization store.

10. The program protection apparatus of Claim 9 wherein said program authorization store is a non-volatile store which retains the state of said program authorization identifiers when power is turned off and on.

11. The program protection apparatus of Claim 9 wherein said detection means includes means for addressing said program authorization store with said program name to obtain the program authorization identifier corresponding to the program name.

12. In a computer system adapted for receiving computer programs from a flex-disc, the program protection apparatus comprising,

disc detection apparatus for sensing when a disc has been newly placed in the system,

means for generating an initiation signal for initiating a check as to whether or not the installed disc is an authorized disc,

means for sensing the timing tracks for the disc for sensing the presence of a master disc indicator to provide a master signal whenever the disc is a master,

means for interrogating a master disc which has been newly placed in the system to determine whether or not the disc is a virgin,

means for storing a system identifier on a virgin master disc,

means for checking stored systems identifiers on newly installed discs to provide an authorization signal enabling the disc to be accessed normally by said system if the disc stores the system identifier.

13. A computer system substantially as described herein with reference to the accompanying drawings.

Printed for Her Majesty's Stationery Office by the Courier Press, Leamington Spa, 1984. Published by the Patent Office, 25 Southampton Buildings, London, WC2A 1AY, from which copies may be obtained.